(4)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-232450
(43)Date of publication of application : 16.08.2002

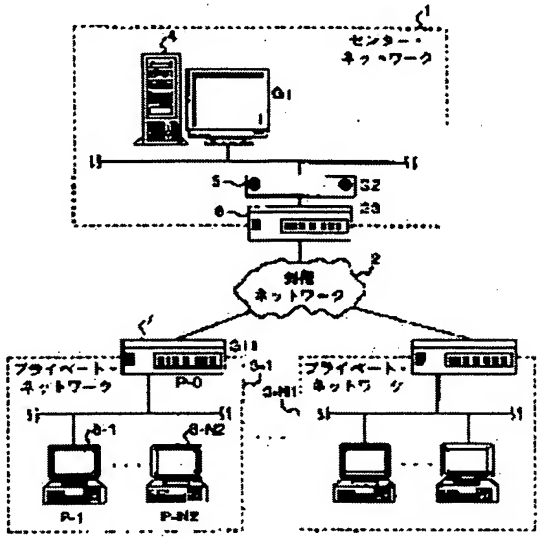
(51)Int.Cl. H04L 12/46
H04L 12/22
H04L 12/66

(21)Application number : 2001-024824
(22)Date of filing : 31.01.2001

(71)Applicant : FURUKAWA ELECTRIC CO LTD:THE
(72)Inventor : NANBA MIKAKO

(54) NETWORK REPEATER, DATA COMMUNICATION SYSTEM, DATA COMMUNICATION METHOD AND PROGRAM MAKING COMPUTER PERFORM THE METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To facilitate the mounting and management of a function performing IPSec communication inside and outside a private network and to reduce the cost.
SOLUTION: A network repeater 7 performs the repeating processing of a packet between the private network 3-1 and an outer network 2, where unique private addresses are used in self-private networks. The repeater has a first repeating part encapsulating an ESP packet transmitted within the private network 3-1 into a UDP packet and repeating it to the outer network 2 and a second repeating part decapsulating the UDP packet from the outer network 2 into the ESP packet and repeating it into the private network 3-1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－232450
（Ｐ２００２－２３２４５０Ａ）
(43)公開日　平成14年８月16日(2002.8.16)

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ（参考）
H04L 12/46		H04L 12/46	E	5K030
12/22		12/22		5K033
12/66		12/66	B	

審査請求　未請求　請求項の数９　ＯＬ　（全15頁）

(21)出願番号　特願2001－24824(Ｐ2001－24824)

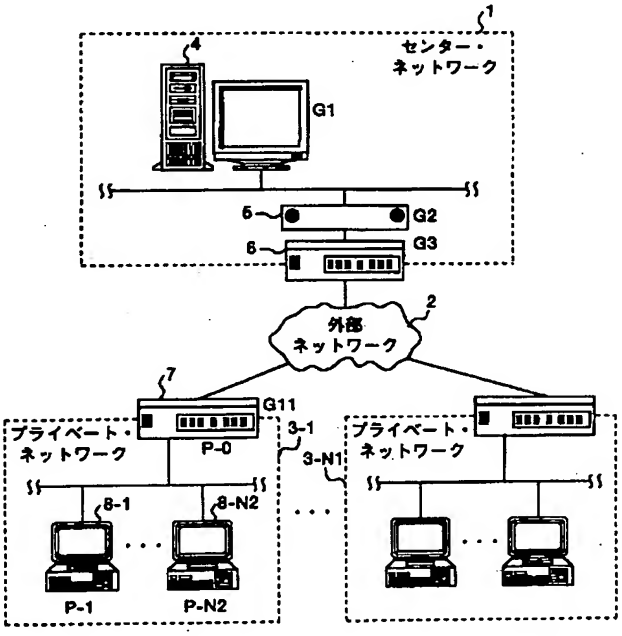
(22)出願日　平成13年１月31日(2001.1.31)

(71)出願人　000005290
古河電気工業株式会社
東京都千代田区丸の内２丁目６番１号
(72)発明者　難波　美香子
東京都千代田区丸の内２丁目６番１号　古河電気工業株式会社内
(74)代理人　100089118
弁理士　酒井　宏明

Ｆターム(参考)　5K030 GA15 HA08 HD03 HD06 JA05 KA02
5K033 AA08 CB08 CB14 CC01 DA06 DB13 DB18

(54)【発明の名称】ネットワーク中継装置、データ通信システム、データ通信方法およびその方法をコンピュータに実行させるプログラム

(57)【要約】
【課題】　プライベートネットワーク内とプライベートネットワーク外とのＩＰＳｅｃ通信を行う機能の実装および管理を容易化し、コストを低減すること。
【解決手段】　自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワーク３－１と外部ネットワーク２との間でパケットの中継処理を行うネットワーク中継装置７において、プライベートネットワーク３－１内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化して外部ネットワーク２に中継する第１中継部と、外部ネットワーク２からのＵＤＰパケットをＥＳＰパケットにデカプセル化してプライベートネットワーク３－１内に中継する第２中継部とを備える。



1

【特許請求の範囲】

【請求項１】　自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でパケットの中継処理を行うネットワーク中継装置において、

前記プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化して前記プライベートネットワーク外に中継する第１中継手段と、

前記プライベートネットワーク外からのＵＤＰパケットをＥＳＰパケットにデカプセル化して前記プライベートネットワーク内に中継する第２中継手段と、

を具備することを特徴とするネットワーク中継装置。

【請求項２】　自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でパケットの中継処理を行うネットワーク中継装置と、前記プライベートネットワーク外に配置されたＩＰＳｅｃ装置と、を備えたデータ通信システムにおいて、

前記ネットワーク中継装置は、

前記プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化して前記ＩＰＳｅｃ装置宛てに中継する第１中継手段と、

前記ＩＰＳｅｃ装置からのＵＤＰパケットをＥＳＰパケットにデカプセル化して前記プライベートネットワーク内に中継する第２中継手段と、

を具備し、

前記ＩＰＳｅｃ装置は、

前記第１中継手段からの前記ＵＤＰパケットをＥＳＰパケットにデカプセル化するデカプセル化手段と、

前記デカプセル化手段がデカプセル化した前記ＥＳＰパケットの受信処理を行うＥＳＰ受信処理手段と、

前記プライベートネットワークにＥＳＰパケットを送信する場合、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信する送信手段と、

を具備することを特徴とするデータ通信システム。

【請求項３】　前記ネットワーク中継装置は、

前記第１中継手段がカプセル化する前記ＥＳＰパケットの送信元のＵＤＰポート番号を決定する決定手段と、

前記送信元の前記プライベートアドレスおよび前記ＵＤＰポート番号を対応させて記憶する第１記憶手段と、

を具備し、

前記ＩＰＳｅｃ装置は、前記デカプセル化手段がデカプセル化する前記ＵＤＰパケットのＵＤＰ送信元ポート番号を記憶する第２記憶手段を具備し、

前記第１中継手段は、前記決定手段が決定した前記ＵＤＰポート番号をＵＤＰ送信ポート番号として用いて前記カプセル化を行い、前記第１記憶手段が記憶した前記ＵＤＰポート番号をＵＤＰ宛先ポート番号とするＵＤＰパケットを前記第２中継手段が受信した後、該ＵＤＰポート番号に対応する前記送信元からの前記ＥＳＰパケットの前記カプセル化を省略し、

前記第２中継手段は、受信した前記ＵＤＰパケットのＵＤＰ宛先ポート番号に対応する前記プライベートアドレス宛てに前記中継を行い、

前記送信手段は、前記第２記憶手段が記憶した前記ＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用いて前記カプセル化を行うことを特徴とする請求項２に記載のデータ通信システム。

【請求項４】　自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でパケットの中継処理を行うネットワーク中継装置と、前記プライベートネットワーク外に配置されたＩＰＳｅｃ装置と、を備えたデータ通信システムにおいて、

前記ネットワーク中継装置は、

前記プライベートネットワーク内から送信されたＩＫＥネゴシエーション用のＵＤＰパケットを前記ＩＰＳｅｃ装置宛てに中継する場合に該ＵＤＰパケットのＵＤＰ送信元ポート番号を決定して中継する第１中継手段と、

前記ＵＤＰパケットの送信元の前記プライベートアドレスおよび前記ＵＤＰ送信元ポート番号を対応させて記憶する第１記憶手段と、

前記ＩＰＳｅｃ装置からのＵＤＰパケットをＥＳＰパケットにデカプセル化し、該ＵＤＰパケットのＵＤＰ宛先ポート番号に対応する前記プライベートアドレス宛てに中継する第２中継手段と、

前記ＩＰＳｅｃ装置は、

前記第１中継手段からの前記ＵＤＰパケットの前記ＵＤＰ送信元ポート番号を記憶する第２記憶手段と、

前記プライベートネットワークにＥＳＰパケットを送信する場合、前記第２記憶手段が記憶した前記ＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用い、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信する送信手段と、

を具備することを特徴とするデータ通信システム。

【請求項５】　自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でＥＳＰパケットを送受信するデータ通信方法において、

前記プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化して前記プライベートネットワーク外に中継する第１中継工程と、

前記プライベートネットワーク外からのＵＤＰパケットをＥＳＰパケットにデカプセル化して前記プライベートネットワーク内に中継する第２中継工程と、

を含むことを特徴とするデータ通信方法。

【請求項６】　自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でＥＳＰパケットを送受信するデータ通信方法において、
前記プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化して前記プライベートネットワーク外に中継する第１中継工程と、
前記第１中継工程で中継された前記ＵＤＰパケットの宛先側で、該ＵＤＰパケットをＥＳＰパケットにデカプセル化するデカプセル化工程と、
前記デカプセル化工程でデカプセル化された前記ＥＳＰパケットの受信処理を行うＥＳＰ受信処理工程と、
前記宛先側で、前記プライベートネットワークにＥＳＰパケットを送信する場合、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信する送信工程と、
前記送信工程で送信された前記ＵＤＰパケットをＥＳＰパケットにデカプセル化して前記プライベートネットワーク内に中継する第２中継工程と、
を含むことを特徴とするデータ通信方法。
【請求項７】　前記第１中継工程では、前記ＥＳＰパケットの送信元のＵＤＰポート番号を決定し、該ＵＤＰポート番号をＵＤＰ送信元ポート番号として用いて前記カプセル化を行い、該送信元の前記プライベートアドレスおよび該ＵＤＰポート番号を対応させて記憶し、該ＵＤＰポート番号をＵＤＰ宛先ポート番号とするＵＤＰパケットが前記第２中継工程で受信された後、該ＵＤＰポート番号に対応する前記送信元からの前記ＥＳＰパケットの前記カプセル化を省略し、
前記第２中継工程では、受信した前記ＵＤＰパケットのＵＤＰ宛先ポート番号に対応する前記プライベートアドレス宛てに前記中継を行い、
前記デカプセル化工程では、前記デカプセル化する前記ＵＤＰパケットのＵＤＰ送信元ポート番号を記憶し、
前記送信工程では、前記デカプセル化工程で記憶された前記ＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用いて前記カプセル化を行うことを特徴とする請求項６に記載のデータ通信方法。
【請求項８】　自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でＥＳＰパケットを送受信するデータ通信方法において、
前記プライベートネットワーク内から送信されたＩＫＥネゴシエーション用のＵＤＰパケットを該プライベートネットワーク外に中継する場合、該ＵＤＰパケットのＵＤＰ送信元ポート番号を決定し、該ＵＤＰパケットの送信元の前記プライベートアドレスおよび該ＵＤＰ送信元ポート番号を対応させて記憶する第１中継工程と、
前記第１中継工程で中継された前記ＵＤＰパケットの宛先側で、該ＵＤＰパケットの前記ＵＤＰ送信元ポート番号を記憶する記憶工程と、
前記宛先側で、前記プライベートネットワークにＥＳＰパケットを送信する場合、前記記憶工程で記憶された前記ＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用い、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信する送信工程と、
前記送信工程で送信された前記ＵＤＰパケットをＥＳＰパケットにデカプセル化し、該ＵＤＰパケットの前記ＵＤＰ宛先ポートに対応する前記プライベートアドレス宛てに中継する第２中継工程と、
を含むことを特徴とするデータ通信方法。
【請求項９】　請求項５～８のいずれか一つに記載された方法をコンピュータに実行させるプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、プライベートなアドレスを用いるプライベートネットワークとプライベートネットワーク外の外部ネットワークとの間でＩＰＳｅｃ通信を行うネットワーク中継装置、データ通信システム、データ通信方法およびその方法をコンピュータに実行させるプログラムに関する。
【０００２】
【従来の技術】ＩＰ（Internet Protocol）による通信では、ネットワーク上の各装置に対して固有のＩＰアドレスを割り付け、これらのＩＰアドレスを各装置の識別子として用いる。詳細には、送信データ内のＩＰヘッダに宛先および送信元のＩＰアドレス情報を格納することによって、データを正しい宛先に転送するとともにデータの送信元を通知する。インターネット（The Internet）等のパブリックな開かれたネットワークでは、ＩＰアドレスが重複しないように、全世界で唯一となるグローバルＩＰアドレスが使用される。
【０００３】しかし、プライベートな閉じたネットワーク（以下、プライベートネットワークと呼ぶ）では、グローバルＩＰアドレスを節約するために、該プライベートネットワーク内でのみ重複しないプライベートＩＰアドレスを使用することができる。プライベートネットワークでは、インターネット等の外部のネットワークとの通信を行う場合、ＴＣＰ（Transmission Control Protocol）／ＵＤＰ（UserDatagram Protocol）およびＮＡＴ（Network Address Translator）を用い、プライベートネットワークに対して一つ割り当てられたグローバルＩＰアドレスとプライベートＩＰアドレスとのアドレス変換を行う。
【０００４】プライベートネットワーク内の装置から外部のネットワークにデータを送信する場合、プライベートネットワークと外部のネットワークとを接続するルータは、中継するデータの送信元ＩＰアドレスをプライベートＩＰアドレスからグローバルＩＰアドレスに変換す

る。また、ルータは、使用中でないＴＣＰ／ＵＤＰポート番号（以下、単にポート番号と呼ぶ）をポート番号プールから選択して送信元ポート番号として決定し、中継データの変換前の送信元ポート番号を、決定した送信元ポート番号に変換する。そして、ルータは、これらのプライベートＩＰアドレス，変換元ポート番号（変換前の送信元ポート番号）および変換後ポート番号（変換後の送信元ポート番号）を対応させて変換テーブルに保持しておく。

【０００５】一方、外部のネットワークからプライベートネットワーク内の装置にデータを送信する場合、ルータは、中継データの宛先ポート番号および変換テーブルに基づいて、その宛先ポート番号に一致する変換後ポート番号に対応するプライベートＩＰアドレスおよび変換元ポート番号を検索し、中継データのグローバルＩＰアドレスおよび宛先ポート番号を検索結果のプライベートＩＰアドレスおよび変換元ポート番号に変換する。このように、一つのグローバルＩＰアドレスを用いてプライベートネットワーク内の各装置とプライベートネットワーク外との通信を行っている。

【０００６】ところで、ＩＰのセキュリティ・プロトコルとして、ＩＰＳｅｃ（IP Security Protocol）が知られている。ＩＰＳｅｃの暗号・認証プロトコルであるＥＳＰ（IP Encapsulating Security Payload）は、ＴＣＰ／ＵＤＰと同じトランスポート層のプロトコルであって、ＴＣＰ／ＵＤＰを使用せず、ポート番号によるアドレス変換を行わない。すなわち、プライベートネットワーク内とプライベートネットワーク外とのＩＰＳｅｃ通信を行うことができないという不具合がある。

【０００７】この不具合を解決する従来の通信方法として、プライベートネットワーク内の各ＩＰＳｅｃ装置（ＩＰＳｅｃ通信を行う装置）がＥＳＰパケットをＵＤＰパケットにカプセル化して送信する通信方法が知られている。この通信方法では、プライベートネットワーク内の各ＩＰＳｅｃ装置に対し、ＥＳＰパケットをＵＤＰパケットにカプセル化させるプログラムをユーザがインストールし、このプログラムに従って各ＩＰＳｅｃ装置がＥＳＰパケットをＵＤＰパケットにカプセル化して送信する。これにより、ポート番号によるアドレス変換がルータで可能になり、プライベートネットワーク内とプライベートネットワーク外とのＩＰＳｅｃ通信が可能となる。

【０００８】

【発明が解決しようとする課題】しかしながら、上述した技術によれば、プライベートネットワーク内の各ＩＰＳｅｃ装置がＥＳＰパケットをＵＤＰパケットにカプセル化するため、プライベートネットワーク内とプライベートネットワーク外とのＩＰＳｅｃ通信を行う機能の実装に手間がかかり、また、ＩＰＳｅｃ装置ごとに該機能の管理を行わなければならず、コストが上昇するという問題点があった。

【０００９】この発明は上記に鑑みてなされたものであって、プライベートネットワーク内とプライベートネットワーク外とのＩＰＳｅｃ通信を行う機能の実装および管理を容易化し、コストを低減することを目的とする。

【００１０】

【課題を解決するための手段】上記の目的を達成するために、請求項１にかかるネットワーク中継装置は、自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でパケットの中継処理を行うネットワーク中継装置において、前記プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化して前記プライベートネットワーク外に中継する第１中継手段と、前記プライベートネットワーク外からのＵＤＰパケットをＥＳＰパケットにデカプセル化して前記プライベートネットワーク内に中継する第２中継手段と、を具備するものである。

【００１１】この請求項１のネットワーク中継装置にあっては、第１中継手段が、プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化してプライベートネットワーク外に中継し、第２中継手段が、プライベートネットワーク外からのＵＤＰパケットをＥＳＰパケットにデカプセル化してプライベートネットワーク内に中継する。これにより、ＥＳＰパケット／ＵＤＰパケットのカプセル化およびデカプセル化をネットワーク中継装置でまとめて行うことができる。

【００１２】また、請求項２にかかるデータ通信システムは、自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でパケットの中継処理を行うネットワーク中継装置と、前記プライベートネットワーク外に配置されたＩＰＳｅｃ装置と、を備えたデータ通信システムにおいて、前記ネットワーク中継装置は、前記プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化して前記ＩＰＳｅｃ装置宛てに中継する第１中継手段と、前記ＩＰＳｅｃ装置からのＵＤＰパケットをＥＳＰパケットにデカプセル化して前記プライベートネットワーク内に中継する第２中継手段と、を具備し、前記ＩＰＳｅｃ装置は、前記第１中継手段からの前記ＵＤＰパケットをＥＳＰパケットにデカプセル化するデカプセル化手段と、前記デカプセル化手段がデカプセル化した前記ＥＳＰパケットの受信処理を行うＥＳＰ受信処理手段と、前記プライベートネットワークにＥＳＰパケットを送信する場合、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信する送信手段と、を具備するものである。

【００１３】この請求項２のデータ通信システムにあっては、第１中継手段が、プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化してＩＰＳｅｃ装置宛てに中継し、第２中継手段が、ＩＰＳｅｃ装置からのＵＤＰパケットをＥＳＰパケットにデカプセル化してプライベートネットワーク内に中継し、デカプセル化手段が、第１中継手段からのＵＤＰパケットをＥＳＰパケットにデカプセル化し、ＥＳＰ受信処理手段が、デカプセル化手段がデカプセル化したＥＳＰパケットの受信処理を行い、送信手段が、プライベートネットワークにＥＳＰパケットを送信する場合、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信する。これにより、ＥＳＰパケット／ＵＤＰパケットのカプセル化およびデカプセル化をネットワーク中継装置でまとめて行うことができる。

【００１４】また、請求項３にかかるデータ通信システムは、請求項２に記載のデータ通信システムにおいて、前記ネットワーク中継装置が、前記第１中継手段がカプセル化する前記ＥＳＰパケットの送信元のＵＤＰポート番号を決定する決定手段と、前記送信元の前記プライベートアドレスおよび前記ＵＤＰポート番号を対応させて記憶する第１記憶手段と、を具備し、前記第１中継手段が、前記決定手段が決定した前記ＵＤＰポート番号をＵＤＰ送信ポート番号として用いて前記カプセル化を行い、前記第１記憶手段が記憶した前記ＵＤＰポート番号をＵＤＰ宛先ポート番号とするＵＤＰパケットを前記第２中継手段が受信した後、該ＵＤＰポート番号に対応する前記送信元からの前記ＥＳＰパケットの前記カプセル化を省略し、前記第２中継手段が、受信した前記ＵＤＰパケットのＵＤＰ宛先ポート番号に対応する前記プライベートアドレス宛てに前記中継を行い、前記ＩＰＳｅｃ装置が、前記デカプセル化手段がデカプセル化する前記ＵＤＰパケットのＵＤＰ送信元ポート番号を記憶する第２記憶手段を具備し、前記送信手段が、前記第２記憶手段が記憶した前記ＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用いて前記カプセル化を行うものである。

【００１５】この請求項３のデータ通信システムにあっては、決定手段が、第１中継手段がカプセル化するＥＳＰパケットの送信元のＵＤＰポート番号を決定し、第１記憶手段が、送信元のプライベートアドレスおよびＵＤＰポート番号を対応させて記憶し、第１中継手段が、決定手段が決定したＵＤＰポート番号をＵＤＰ送信ポート番号として用いてカプセル化を行い、第１記憶手段が記憶したＵＤＰポート番号をＵＤＰ宛先ポート番号とするＵＤＰパケットを第２中継手段が受信した後、該ＵＤＰポート番号に対応する送信元からのＥＳＰパケットのカプセル化を省略し、第２中継手段が、受信したＵＤＰパケットのＵＤＰ宛先ポート番号に対応するプライベートアドレス宛てに中継を行い、第２記憶手段が、デカプセル化手段がデカプセル化するＵＤＰパケットのＵＤＰ送信元ポート番号を記憶し、送信手段が、第２記憶手段が記憶したＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用いてカプセル化を行う。これにより、同一の送信元からのＥＳＰパケットのカプセル化を２回目以降省略して、ＵＤＰパケットへのカプセル化によるオーバヘッドを低減することができる。

【００１６】また、請求項４にかかるデータ通信システムは、自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でパケットの中継処理を行うネットワーク中継装置と、前記プライベートネットワーク外に配置されたＩＰＳｅｃ装置と、を備えたデータ通信システムにおいて、前記ネットワーク中継装置は、前記プライベートネットワーク内から送信されたＩＫＥネゴシエーション用のＵＤＰパケットを前記ＩＰＳｅｃ装置宛てに中継する場合に該ＵＤＰパケットのＵＤＰ送信元ポート番号を決定して中継する第１中継手段と、前記ＵＤＰパケットの送信元の前記プライベートアドレスおよび前記ＵＤＰ送信元ポート番号を対応させて記憶する第１記憶手段と、前記ＩＰＳｅｃ装置からのＵＤＰパケットをＥＳＰパケットにデカプセル化し、該ＵＤＰパケットのＵＤＰ宛先ポート番号に対応する前記プライベートアドレス宛てに中継する第２中継手段と、前記ＩＰＳｅｃ装置は、前記第１中継手段からの前記ＵＤＰパケットの前記ＵＤＰ送信元ポート番号を記憶する第２記憶手段と、前記プライベートネットワークにＥＳＰパケットを送信する場合、前記第２記憶手段が記憶した前記ＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用い、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信する送信手段と、を具備するものである。

【００１７】この請求項４のデータ通信システムにあっては、第１中継手段が、プライベートネットワーク内から送信されたＩＫＥネゴシエーション用のＵＤＰパケットをＩＰＳｅｃ装置宛てに中継する場合に該ＵＤＰパケットのＵＤＰ送信元ポート番号を決定して中継し、第１記憶手段が、ＵＤＰパケットの送信元のプライベートアドレスおよびＵＤＰ送信元ポート番号を対応させて記憶し、第２中継手段が、ＩＰＳｅｃ装置からのＵＤＰパケットをＥＳＰパケットにデカプセル化し、該ＵＤＰパケットのＵＤＰ宛先ポート番号に対応するプライベートアドレス宛てに中継し、第２記憶手段が、第１中継手段からのＵＤＰパケットのＵＤＰ送信元ポート番号を記憶し、送信手段が、プライベートネットワークにＥＳＰパケットを送信する場合、第２記憶手段が記憶したＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用い、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信する。これにより、ＵＤＰパケットからＥＳＰパケットへのデカプセル化をネットワーク中継装置でまとめて

行うことができ、また、プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化する必要がなくなる。

【００１８】また、請求項５にかかるデータ通信方法は、自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でＥＳＰパケットを送受信するデータ通信方法において、前記プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化して前記プライベートネットワーク外に中継する第１中継工程と、前記プライベートネットワーク外からのＵＤＰパケットをＥＳＰパケットにデカプセル化して前記プライベートネットワーク内に中継する第２中継工程と、を含むものである。

【００１９】この請求項５のデータ通信方法にあっては、第１中継工程で、プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化してプライベートネットワーク外に中継し、第２中継工程で、プライベートネットワーク外からのＵＤＰパケットをＥＳＰパケットにデカプセル化してプライベートネットワーク内に中継する。これにより、ＥＳＰパケット／ＵＤＰパケットのカプセル化およびデカプセル化をまとめて行うことができる。

【００２０】また、請求項６にかかるデータ通信方法は、自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でＥＳＰパケットを送受信するデータ通信方法において、前記プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化して前記プライベートネットワーク外に中継する第１中継工程と、前記第１中継工程で中継された前記ＵＤＰパケットの宛先側で、該ＵＤＰパケットをＥＳＰパケットにデカプセル化するデカプセル化工程と、前記デカプセル化工程でデカプセル化された前記ＥＳＰパケットの受信処理を行うＥＳＰ受信処理工程と、前記宛先側で、前記プライベートネットワークにＥＳＰパケットを送信する場合、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信する送信工程と、前記送信工程で送信された前記ＵＤＰパケットをＥＳＰパケットにデカプセル化して前記プライベートネットワーク内に中継する第２中継工程と、を含むものである。

【００２１】この請求項６のデータ通信方法にあっては、第１中継工程で、プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化してプライベートネットワーク外に中継し、デカプセル化工程で、第１中継工程で中継されたＵＤＰパケットの宛先側で該ＵＤＰパケットをＥＳＰパケットにデカプセル化し、ＥＳＰ受信処理工程で、デカプセル化工程でデカプセル化されたＥＳＰパケットの受信処理を行い、送信工程で、宛先側からプライベートネットワークにＥＳＰパケットを送信する場合、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信し、第２中継工程で、送信工程で送信されたＵＤＰパケットをＥＳＰパケットにデカプセル化してプライベートネットワーク内に中継する。これにより、ＥＳＰパケット／ＵＤＰパケットのカプセル化およびデカプセル化をまとめて行うことができる。

【００２２】また、請求項７にかかるデータ通信方法は、請求項６に記載のデータ通信方法において、前記第１中継工程では、前記ＥＳＰパケットの送信元のＵＤＰポート番号を決定し、該ＵＤＰポート番号をＵＤＰ送信元ポート番号として用いて前記カプセル化を行い、該送信元の前記プライベートアドレスおよび該ＵＤＰポート番号を対応させて記憶し、該ＵＤＰポート番号をＵＤＰ宛先ポート番号とするＵＤＰパケットが前記第２中継工程で受信された後、該ＵＤＰポート番号に対応する前記送信元からの前記ＥＳＰパケットの前記カプセル化を省略し、前記第２中継工程では、受信した前記ＵＤＰパケットのＵＤＰ宛先ポート番号に対応する前記プライベートアドレス宛てに前記中継を行い、前記デカプセル化工程では、前記デカプセル化する前記ＵＤＰパケットのＵＤＰ送信元ポート番号を記憶し、前記送信工程では、前記デカプセル化工程で記憶された前記ＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用いて前記カプセル化を行うものである。

【００２３】この請求項７のデータ通信方法にあっては、第１中継工程で、ＥＳＰパケットの送信元のＵＤＰポート番号を決定し、該ＵＤＰポート番号をＵＤＰ送信元ポート番号として用いてカプセル化を行い、該送信元のプライベートアドレスおよび該ＵＤＰポート番号を対応させて記憶し、該ＵＤＰポート番号をＵＤＰ宛先ポート番号とするＵＤＰパケットが第２中継工程で受信された後、該ＵＤＰポート番号に対応する送信元からのＥＳＰパケットのカプセル化を省略し、第２中継工程で、受信したＵＤＰパケットのＵＤＰ宛先ポート番号に対応するプライベートアドレス宛てに中継を行い、デカプセル化工程で、デカプセル化するＵＤＰパケットのＵＤＰ送信元ポート番号を記憶し、送信工程で、デカプセル化工程で記憶されたＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用いてカプセル化を行う。これにより、同一の送信元からのＥＳＰパケットのカプセル化を２回目以降省略して、ＵＤＰパケットへのカプセル化によるオーバヘッドを低減することができる。

【００２４】また、請求項８にかかるデータ通信方法は、自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でＥＳＰパケットを送受信するデータ通信方法におい

て、前記プライベートネットワーク内から送信されたＩＫＥネゴシエーション用のＵＤＰパケットを該プライベートネットワーク外に中継する場合、該ＵＤＰパケットのＵＤＰ送信元ポート番号を決定し、該ＵＤＰパケットの送信元の前記プライベートアドレスおよび該ＵＤＰ送信元ポート番号を対応させて記憶する第１中継工程と、前記第１中継工程で中継された前記ＵＤＰパケットの宛先側で、該ＵＤＰパケットの前記ＵＤＰ送信元ポート番号を記憶する記憶工程と、前記宛先側で、前記プライベートネットワークにＥＳＰパケットを送信する場合、前記記憶工程で記憶された前記ＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用い、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信する送信工程と、前記送信工程で送信された前記ＵＤＰパケットをＥＳＰパケットにデカプセル化し、該ＵＤＰパケットの前記ＵＤＰ宛先ポートに対応する前記プライベートアドレス宛てに中継する第２中継工程と、を含むものである。

【００２５】この請求項８のデータ通信方法にあっては、第１中継工程で、プライベートネットワーク内から送信されたＩＫＥネゴシエーション用のＵＤＰパケットを該プライベートネットワーク外に中継する場合、該ＵＤＰパケットのＵＤＰ送信元ポート番号を決定し、該ＵＤＰパケットの送信元のプライベートアドレスおよび該ＵＤＰ送信元ポート番号を対応させて記憶し、記憶工程で、第１中継工程で中継されたＵＤＰパケットの宛先側で、該ＵＤＰパケットのＵＤＰ送信元ポート番号を記憶し、送信工程で、宛先側からプライベートネットワークにＥＳＰパケットを送信する場合、記憶工程で記憶されたＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用い、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信し、第２中継工程で、送信工程で送信されたＵＤＰパケットをＥＳＰパケットにデカプセル化し、該ＵＤＰパケットのＵＤＰ宛先ポートに対応するプライベートアドレス宛てに中継する。これにより、ＵＤＰパケットからＥＳＰパケットへのデカプセル化をまとめて行うことができ、また、プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化する必要がなくなる。

【００２６】また、請求項９にかかるプログラムは、請求項５～８のいずれか一つに記載された方法をコンピュータに実行させるものである。これにより、請求項５～８のいずれか一つに記載された方法の動作をコンピュータによって実現することが可能となる。

【００２７】ここで、「プログラム」とは、データ処理方法を記述したものであって、記述する言語や記述方法は特に限定されず、ソースコード，バイナリコード，実行形式等の形式を問わない。なお、「プログラム」は必ずしも単一に構成されるものに限られず、複数のモジュールやライブラリとして分散構成されるものや、ＯＳ等の別個のプログラムと協働してその機能を達成するものを含む。

【００２８】

【発明の実施の形態】以下に、この発明の実施の形態を、添付の図面を参照して詳細に説明する。なお、この実施の形態によってこの発明が限定されるものではない。図１は、この発明の一実施の形態にかかる通信ネットワークのシステム構成を示す説明図である。この実施の形態の通信ネットワークは、センターネットワーク１と、複数のプライベートネットワーク３－１～３－Ｎ１と、センターネットワーク１およびプライベートネットワーク３－１～３－Ｎ１を接続するインターネット等の外部ネットワーク２とを備える。外部ネットワーク２は、全世界の不特定多数のネットワークと繋がるグローバル・ネットワークである。

【００２９】各プライベートネットワーク３－１～３－Ｎ１は、全て同様の構成であって、外部ネットワーク２に接続するルータと、複数のＩＰＳｅｃ装置とを有する。各ＩＰＳｅｃ装置は、自プライベートネットワーク内でのみユニークなプライベートＩＰアドレスを用いて通信を行う。各プライベートネットワークは、グローバルＩＰアドレスを一つ有する。この例では、プライベートネットワーク３－１が、ルータ７（グローバルＩＰアドレスＧ１１，プライベートＩＰアドレスＰ－０）とＩＰＳｅｃ装置８－１～８－Ｎ２（プライベートＩＰアドレスＰ－１～Ｐ－Ｎ２）とを備える。

【００３０】ただし、Ｎ１およびＮ２は、任意の数である。センターネットワーク１は、センターネットワーク１外の装置によるアクセスを受けるデータベース・サーバ等のサーバ４（グローバルＩＰアドレスＧ１）と、外部ネットワーク２に接続するルータ６と、ルータ６（グローバルＩＰアドレスＧ３）とサーバ４との間に設けたＩＰＳｅｃ装置５（グローバルＩＰアドレスＧ２）とを備える。

【００３１】たとえば、ＩＰＳｅｃ装置５とＩＰＳｅｃ装置８－１とがＩＰＳｅｃ通信を行う場合、まず、暗号鍵交換を行うＩＫＥ（Internet Key Exchange）ネゴシエーションをこれらのＩＰＳｅｃ装置間で行い、その後、ＥＳＰプロトコルに基づいて、ＩＰＳｅｃ装置８－１からＩＰＳｅｃ装置５宛てにＥＳＰパケットを送信し、ＩＰＳｅｃ装置５からＩＰＳｅｃ装置８－１宛てにＥＳＰパケットを送信する。なお、端末装置であるＩＰＳｅｃ装置８－１～８－Ｎ２に代えて、中継装置であるＩＰＳｅｃ装置を設け、各ＩＰＳｅｃ装置に複数の端末装置を接続してもよい。また、センターネットワークを複数設けてもよいし、各センターネットワーク内に複数のサーバを設けてもよい。

【００３２】つぎにルータ７の機能構成について説明する。図２は、図１に示したルータ７の機能構成を示すブロック図である。ルータ７は、外部ネットワーク２との通信を行うインターフェース部１１と、プライベートネ

ットワーク３－１内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化して外部ネットワーク２に中継する第１中継部１２と、この発明のＮＡＴ変換に用いる変換情報を記憶する記憶部１３と、外部ネットワーク２からのＵＤＰパケットをＥＳＰパケットにデカプセル化してプライベートネットワーク３－１内に中継する第２中継部１４と、プライベートネットワーク３－１内との通信を行うインターフェース部１５とを備える。

【００３３】第１中継部１２は、ＵＤＰパケットの送信元ＵＤＰポート番号（以下、単に送信元ポート番号と呼ぶ）を決定する決定部１６を有し、プライベートネットワーク３－１内のＩＰＳｅｃ装置８－１～８－Ｎ２からのＥＳＰパケットをＵＤＰパケットにカプセル化して外部ネットワーク２に中継する。また、第１中継部１２は、決定部１６が決定した送信元ポート番号とＥＳＰパケットの送信元プライベートＩＰアドレスとを対応させた変換情報を記憶部１３に格納する。記憶部１３は、ハードディスク等の記録媒体を有し、変換情報を記憶する。第２中継部１４は、記憶部１３の変換情報を参照し、外部ネットワーク２からのＵＤＰパケットをＥＳＰパケットにデカプセル化してプライベートネットワーク３－１内に中継する。

【００３４】つぎに、ＩＰＳｅｃ装置５の機能構成について説明する。図３は、図１に示したＩＰＳｅｃ装置５の機能構成を示すブロック図である。ＩＰＳｅｃ装置５は、センターネットワーク１内との通信を行うインターフェース部２１と、ルータ６に接続するインターフェース部２７と、外部ネットワーク２からのＵＤＰパケットをＥＳＰパケットにデカプセル化するデカプセル化部２４と、デカプセル化部２４がデカプセル化したＥＳＰパケットのＥＳＰ受信処理を行うＥＳＰ受信処理部２２と、センターネットワーク１内から送信されたオリジナルＩＰパケットを暗号化してＥＳＰパケットを生成するＥＳＰパケット生成部２３と、ＥＳＰパケット生成部２３が生成したＥＳＰパケットをＵＤＰパケットにカプセル化して外部ネットワーク２に送信する送信部２６と、この発明のＮＡＴ変換に用いる変換情報を記憶する記憶部２５とを備える。

【００３５】デカプセル化部２４は、外部ネットワーク２からのＵＤＰパケットを受信すると、そのＵＤＰパケットの送信元ポート番号を変換情報として記憶部２５に格納するとともに、そのＵＤＰパケットをＥＳＰパケットにデカプセル化する。ＥＳＰ受信処理部２２は、デカプセル化部２４がデカプセル化したＥＳＰパケットのＥＳＰ受信処理を行う。すなわち、ＥＳＰ受信処理部２２は、ＥＳＰパケットに含まれる暗号化されたオリジナルＩＰパケットを復号化し、復号化されたオリジナルＩＰパケットをセンターネットワーク１内に送信する。

【００３６】ＥＳＰパケット生成部２３は、センターネットワーク１内のサーバ４からのオリジナルＩＰパケットを暗号化してＥＳＰパケットを生成する。送信部２６は、記憶部２５の変換情報を参照し、ＥＳＰパケット生成部２３が生成したＥＳＰパケットをＵＤＰパケットにカプセル化して外部ネットワーク２に送信する。記憶部２５は、ハードディスク等の記録媒体を有し、変換情報を記憶する。なお、この例では、ルータ７にＥＳＰパケット／ＵＤＰパケットのカプセル化およびデカプセル化の機能を持たしているが、ルータ７とＩＰＳｅｃ装置８－１～８－Ｎ２との間に該機能を達成する装置を設けてもよい。また、この例では、ＩＰＳｅｃ装置５とルータ６とを別体に設けているが、これらを一体に設けてもよい。また、ＩＰＳｅｃ装置５とサーバ４とを一体に設けてもよい。

【００３７】さて、これまで、ルータ７およびＩＰＳｅｃ装置５の構成について説明したが、ルータ７およびＩＰＳｅｃ装置５の各構成要素は機能概念的なものであり、必ずしも物理的に図示したように構成されていなくてもよい。たとえば、ルータ７およびＩＰＳｅｃ装置５が備える処理機能のうち全部または一部を、図示しないＣＰＵ（Central Processing Unit）およびこのＣＰＵにて解釈実行されるプログラムによって実現することができる。すなわち、図示しないＲＯＭには、ＯＳ（Operating System）等と協働してＣＰＵに命令を与え、ＣＰＵに各種処理を行わせるコンピュータプログラムが格納されている。そして、ＣＰＵは、このプログラムに従って各種処理を行う。また、ルータ７およびＩＰＳｅｃ装置５が備える処理機能のうち全部または一部を、ワイヤードロジックによるハードウェアとして実現することも可能である。

【００３８】以上の構成において、この実施の形態の動作についてフローチャートを参照して説明する。図４は、この実施の形態にかかるルータ７が外部ネットワーク２にパケットを送信する場合の動作手順を示すフローチャートである。ルータ７では、プライベートネットワーク３－１内から送信されたプライベートネットワーク３－１外宛てのパケットをインターフェース部１５が受信すると、まず、第１中継部１２が、そのパケットがＥＳＰパケットであるか否かを判定する（Ｓ１）。図５は、プライベートネットワーク内のＩＰＳｅｃ装置が送信するＥＳＰパケットを含むＩＰパケットの一例を示す説明図である。

【００３９】ここでは、ＩＰＳｅｃ装置８－１によるサーバ４宛てのパケットの例を示している。このパケットでは、オリジナルＩＰパケットを暗号化し、ＥＳＰヘッダを付加し、さらにＩＰヘッダを付加している。このＩＰヘッダの宛先アドレスは、ＩＰＳｅｃ装置５のグローバルＩＰアドレスであり、送信元アドレスはＩＰＳｅｃ装置３－１のプライベートＩＰアドレスである。なお、ここでは、オリジナルＩＰパケットの送信元アドレスとしてＩＰＳｅｃ装置８－１のプライベートＩＰアドレス

Ｐ－１を用いているが、プライベートＩＰアドレスをプライベートネットワーク３－１の外部に出したくない場合は、プライベートＩＰアドレスに代えて他の識別子を用いてもよい。

【００４０】ステップＳ１で、受信パケットがＥＳＰパケットである場合、第１中継部１２は、そのＥＳＰパケットを含むＩＰパケットのＩＰヘッダから、送信元アドレスとして格納されているプライベートＩＰアドレスを取得し、記憶部１３を参照し、そのプライベートＩＰアドレスを含む変換情報が記憶されているか否かを判定する（Ｓ２）。図６は、この実施の形態にかかる変換情報の一例を示す説明図である。図６に示すように、変換情報は、ＥＳＰパケットの送信元のプライベートＩＰアドレスと該送信元に割り当てられたポート番号（ＵＤＰポート番号）とを対応させたものである。この例では、プライベートＩＰアドレスＰ－１とポート番号Ｘ－１が対応し、プライベートＩＰアドレスＰ－２とポート番号Ｘ－２が対応する。

【００４１】ステップＳ２で、受信パケットの送信元に対応する変換情報が記憶部１３に記憶されてない場合、決定部１６は、記憶部１３に記憶されたＮＡＴ変換用のポート番号プールの中から使用中でないポート番号を選択し、該送信元のポート番号として決定する（Ｓ３）。つぎに、第１中継部１２は、決定部１６が決定したポート番号と送信元のプライベートＩＰアドレスとを対応させた変換情報を記憶部１３に格納する（Ｓ４）。つぎに、第１中継部１２は、受信パケットのＩＰヘッダのＮＡＴ変換を行う（Ｓ５）。すなわち、第１中継部１２は、図７に示すように、ＩＰヘッダの送信元アドレスを、プライベートＩＰアドレスからグローバルＩＰアドレスＧ１１に変換する。

【００４２】つぎに、第１中継部１２は、予め取り決めたＵＤＰパケットカプセル化処理用のポート番号Ｘ０をＵＤＰヘッダの宛先ポート番号として用い、ステップＳ３で決定したポート番号をＵＤＰヘッダの送信元ポート番号として用いて、受信ＩＰパケットをＵＤＰパケットにカプセル化する（Ｓ６）。つぎに、グローバルＩＰアドレスＧ１１を送信元アドレスとし、グローバルＩＰアドレスＧ２を宛先アドレスとするＩＰヘッダをＵＤＰパケットに付加し、図８に示すようなＩＰパケットを生成する（Ｓ７）。そして、生成したデータを、インターフェース部１１を介して外部ネットワーク２に送信する（Ｓ８）。

【００４３】一方、ステップＳ１で、受信パケットがＥＳＰパケットでなかった場合、第１中継部１２は、前述した従来と同様のＮＡＴ変換処理を行い（Ｓ９）、ステップＳ８に進む。また、ステップＳ２で、受信したＥＳＰパケットの送信元に対応する変換情報がすでに記憶部１３に記憶されていた場合、第１中継部１２は、ステップＳ５と同様のＩＰヘッダのＮＡＴ変換処理を行い、ステップＳ８に進む。すなわち、プライベートネットワーク３－１内の同一のＩＰＳｅｃ装置からのＥＳＰパケットを受信した場合、ＵＤＰパケットへのカプセル化を２回目以降は省略する。

【００４４】あるいは、プライベートネットワーク３－１内のＩＰＳｅｃ装置からのＩＰＳｅｃ装置５宛てのパケットを一度中継し、ＩＰＳｅｃ装置５からプライベートネットワーク３－１内の該ＩＰＳｅｃ装置宛てのパケットを受信したあと、ＵＤＰパケットへのカプセル化の省略を行うようにしてもよい。この方法によれば、ＵＤＰパケットへのカプセル化を最初の一度だけ行えばよく、あとは省略できるため、ＩＰヘッダの２０バイトおよびＵＤＰヘッダの８バイトのオーバヘッドを低減することができる。

【００４５】また、ＵＤＰパケットへのカプセル化を一度行ったあと、所定時間以上、その送信元のＩＰＳｅｃ装置宛てまたは該ＩＰＳｅｃ装置からのＥＳＰパケットの中継がなかった場合、該ＩＰＳｅｃ装置に対応する変換情報を開放し、使用していたポート番号をポート番号プールに戻してもよい。これにより、変換情報用のメモリ領域を低減することができる。この場合、該ＩＰＳｅｃ装置が再びＥＳＰパケットをＩＰＳｅｃ装置５宛てに送信するときに、再びポート番号の取得が行われる。

【００４６】つぎに、ＩＰＳｅｃ装置５が外部ネットワーク２からのパケットを受信する場合の動作について説明する。図９は、この実施の形態にかかるＩＰＳｅｃ装置５が外部ネットワーク２からのパケットを受信する場合の動作手順を示すフローチャートである。ＩＰＳｅｃ装置５では、外部ネットワーク２からのパケットをルータ６を介してインターフェース部２７が受信すると、まず、デカプセル化部２４が、自装置宛てのパケットか否かを判定する（Ｓ１１）。受信パケットが自装置宛てであった場合、デカプセル化部２４は、該パケットが宛先ポート番号Ｘ０のＵＤＰパケットであるか否かを判定する（Ｓ１２）。

【００４７】受信パケットが宛先ポート番号Ｘ０のＵＤＰパケットである場合、デカプセル化部２４は、そのＵＤＰパケットをＥＳＰパケットにデカプセル化する（Ｓ１３）。すなわち、デカプセル化部２４は、受信パケットのＩＰヘッダおよびＵＤＰヘッダを取り除く。つぎに、デカプセル化部２４は、ＵＤＰヘッダの送信元ポート番号を取得し、該送信元ポートと送信元のＩＰＳｅｃ装置とを対応させた変換情報（図１０参照）を記憶部２５に格納する（Ｓ１４）。たとえば、図８に示したパケットを受信した場合は、送信元のＩＰＳｅｃ装置８－１に対応させてポート番号Ｘ－１が記憶部２５に格納される。プライベートネットワークのルータ側でポート番号の開放および再取得が行われた場合、デカプセル化部２４は、記憶部２５に記憶されている送信元ＩＰＳｅｃ装置のポート番号の情報を更新する。

【００４８】また、記憶部２５は、ＩＰＳｅｃ通信の相手装置情報として、相手装置であるＩＰＳｅｃ装置のＩＰアドレスや受信ＥＳＰ識別子等の情報を保持する（図１１参照）。ＥＳＰヘッダには、ＩＫＥネゴシエーションでＩＰＳｅｃ装置同士がお互いに取り決めた識別子が含まれている。この識別子によってＥＳＰパケットの送信元であるＩＰＳｅｃ装置を識別することができる。つぎに、ＥＳＰ受信処理部２２は、ＥＳＰパケットに含まれる暗号化されたオリジナルＩＰパケットを復号化する（Ｓ１５）。そして、ＥＳＰ受信処理部２２は、図１２に示すようなオリジナルＩＰパケットをセンターネットワーク１内に送信する（Ｓ１６）。

【００４９】一方、ステップＳ１１で、受信パケットが自装置宛てでなかった場合、デカプセル化部２４およびＥＳＰ受信処理部２２は、従来の通常の中継装置と同様の中継処理を行う（Ｓ１７）。また、ステップＳ１２で、受信パケットが宛先ポート番号Ｘ０のＵＤＰパケットでなかった場合、デカプセル化部２４およびＥＳＰ受信処理部２２は、受信パケットのプロトコルに応じた従来の通常の受信処理を行う（Ｓ１８）。

【００５０】つぎに、ＩＰＳｅｃ装置５が外部ネットワーク２にパケットを送信する場合の動作について説明する。図１３は、この実施の形態にかかるＩＰＳｅｃ装置５が外部ネットワーク２にパケットを送信する場合の動作手順を示すフローチャートである。ＩＰＳｅｃ装置５では、センターネットワーク１内から送信されたセンターネットワーク１外宛てのパケットをインターフェース部２１が受信すると、まず、ＥＳＰパケット生成部２３が、そのパケットがＩＰＳｅｃ通信の対象であるか否かを判定する（Ｓ２１）。

【００５１】ＩＰＳｅｃ通信の対象であるか否かは、宛先ＩＰアドレスや送信元ＩＰアドレス等のパケットデータに基づいて判定する。記憶部２５は、図１４に示すような、宛先ＩＰアドレス／マスク，送信元ＩＰアドレス／マスク，ＴＣＰ／ＵＤＰ等のプロトコル，宛先ポート番号，送信元ポート番号，送信先装置等のＩＰ通信対象となるパケットの条件を規定したＩＰＳｅｃ通信対象パケット情報を保持する。ＥＳＰパケット生成部２３は、ＩＰＳｅｃ通信対象パケット情報を参照し、受信パケットがＩＰＳｅｃ通信対象パケット情報の条件を満たすか否かに基づいて、そのパケットがＩＰＳｅｃ通信の対象であるか否かを判定する。

【００５２】ステップＳ２１で、受信パケットがＩＰＳｅｃ通信の対象である場合、ＥＳＰパケット生成部２３は、受信パケットであるオリジナルＩＰパケット（図１５参照）を暗号化し、ＥＳＰヘッダを付加してＥＳＰパケットを生成する（Ｓ２２）。つぎに、送信部２６は、記憶部２５を参照し、送信先のＩＰＳｅｃ装置に対応する変換情報が記憶されているか否かを判定する（Ｓ２３）。送信先のＩＰＳｅｃ装置に対応する変換情報が記憶されている場合、送信部２６は、その変換情報のポート番号を取得して宛先ポート番号として用い、予め取り決めたポート番号Ｘ０を送信元ポート番号として用いて、ＥＳＰパケット生成部２３が生成したＥＳＰパケットをＵＤＰパケットにカプセル化する（Ｓ２４）。

【００５３】このように、ＩＰＳｅｃ装置５内でＥＳＰパケットの生成およびＵＤＰパケットへのカプセル化をまとめて行うので、ＥＳＰパケットにＩＰヘッダを付加せずに直接ＵＤＰパケットにカプセル化することができる。つぎに、送信部２６は、送信先のグローバルＩＰアドレスおよび自装置のグローバルＩＰアドレスＧ２の情報を含むＩＰヘッダをＵＤＰパケットに付加し（Ｓ２５）、図１６に示すようなＩＰパケットを生成する。生成されたデータは、ルータ６を介して外部ネットワーク２に送信される（Ｓ２６）。

【００５４】一方、ステップＳ２１で、受信パケットがＩＰＳｅｃ通信の対象でなかった場合、ＥＳＰパケット生成部２３および送信部２６は、従来の通常の中継装置と同様の中継処理を行い（Ｓ２７）、ステップＳ２６に進む。また、ステップＳ２３で、送信先のＩＰＳｅｃ装置に対応する変換情報が記憶部２５に記憶されていなかった場合、ＥＳＰパケット生成部２３および送信部２６は、ＥＳＰパケットにＩＰヘッダを付加し（Ｓ２８）、ステップＳ２６に進む。

【００５５】つぎに、ルータ７が外部ネットワーク２からのＵＤＰパケットを受信する場合の動作について説明する。図１７は、この実施の形態にかかるルータ７が外部ネットワーク２からのＵＤＰパケットを受信する場合の動作手順を示すフローチャートである。ルータ７では、外部ネットワーク２からのＵＤＰパケットをインターフェース部１１が受信すると、まず、第２中継部１４が、受信パケットの宛先ポート番号に対応する変換情報が記憶部１３に記憶されているか否かを判定する（Ｓ３１）。受信パケットの宛先ポート番号に対応する変換情報が記憶部１３に記憶されている場合、第２中継部１４は、受信パケットのＩＰヘッダおよびＵＤＰヘッダを除去し、ＥＳＰパケットにデカプセル化する（Ｓ３２）。

【００５６】つぎに、第２中継部１４は、受信パケットの宛先ポート番号に対応するプライベートＩＰアドレスを変換情報から取得し、このプライベートＩＰアドレスを送信先アドレスとするＩＰヘッダをＥＳＰパケットに付加する（Ｓ３３）。たとえば、図１６に示したパケットを受信した場合、第２中継部１４は、そのパケットをＥＳＰパケットにデカプセル化し、宛先ポート番号Ｘ－１に対応するプライベートＩＰアドレスＰ－１を宛先アドレスとして用い、図１８に示すＩＰパケットを生成する。そして、第２中継部１４は、このＩＰパケットをプライベートネットワーク３－１内に送信する（Ｓ３４）。

【００５７】一方、ステップＳ３１で、受信パケットの

宛先ポート番号に対応する変換情報が記憶部２５に記憶されていない場合、第２中継部１４は、前述した従来のＮＡＴ変換処理を行い（Ｓ３５）、ステップＳ３４に進む。このように、ＵＤＰパケット／ＥＳＰパケットのカプセル化およびデカプセル化をルータ７が行うため、プライベートネットワーク内のＩＰＳｅｃ装置は標準のＩＰＳｅｃ処理を行うだけでプライベートネットワークの外部とのＩＰＳｅｃ通信を行うことができる。

【００５８】さて、前述した例では、プライベートネットワーク内のＩＰＳｅｃ装置によって１回目のＥＳＰパケットを送信する場合に、送信元ポート番号を決定し、ＥＳＰパケットをＵＤＰパケットにカプセル化していた。しかし、ＩＫＥネゴシエーションで使用するパケットはＵＤＰパケットであるので、ＩＫＥネゴシエーションで使用したポート番号を、ＥＳＰパケットの送信元のポート番号として用いてもよい。すなわち、決定部１６は、ＩＫＥネゴシエーションで使用するポート番号を決定し、第１中継部１２は、ＩＫＥネゴシエーションで使用したポート番号およびプライベートＩＰアドレスを変換情報として記憶部１３に格納する。

【００５９】一方、ＩＰＳｅｃ装置５のデカプセル化部２４は、ＩＫＥネゴシエーションで使用したポート番号を、ＩＰＳｅｃ通信相手装置と対応させ、変換情報として記憶部２５に格納する。これによって、プライベートネットワーク内のＩＰＳｅｃ装置がプライベートネットワーク外にＥＳＰパケットを送信する場合、１回目からＵＤＰパケットへのカプセル化を省略することができる。また、前述した例では、センターネットワーク１内でグローバルＩＰアドレスを使用していたが、センターネットワーク１内でプライベートＩＰアドレスを使用してもよい。この場合は、ルータ６がＮＡＴ変換を行う。

【００６０】この実施の形態によれば、第１中継部１２が、プライベートネットワーク３－１内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化して外部ネットワーク２に中継し、第２中継部１４が、外部ネットワーク２からのＵＤＰパケットをＥＳＰパケットにデカプセル化してプライベートネットワーク３－１内に中継する。これにより、ＥＳＰパケット／ＵＤＰパケットのカプセル化およびデカプセル化をルータ７でまとめて行うことができるため、プライベートネットワーク１内とプライベートネットワーク１外とのＩＰＳｅｃ通信を行う機能の実装および管理を容易化し、コストを低減することができる。

【００６１】なお、この実施の形態にかかる通信方法を実現するコンピュータプログラムを、フロッピー（登録商標）ディスク等の磁気ディスク、ＲＯＭ，ＥＰＲＯＭ，ＥＥＰＲＯＭ，フラッシュＲＯＭ等の半導体メモリ（カートリッジ，ＰＣカード等に内蔵されているものを含む）、ＣＤ－ＲＯＭ，ＤＶＤ等の光ディスク、ＭＯ等の光磁気ディスク、等の可搬の記録媒体に格納し、この記録媒体に記録されたプログラムを、ルータ７およびＩＰＳｅｃ装置５に内蔵されるＲＯＭ，ＲＡＭ，ハードディスク等の固定用の記録媒体にインストールすることによって、そのルータ７およびＩＰＳｅｃ装置５に前述した機能を具備させることもできる。

【００６２】また、このプログラムを、ＬＡＮ，ＷＡＮ，インターネット等のネットワークを介して伝送し、伝送されたプログラムをルータ７およびＩＰＳｅｃ装置５の固定用の記録媒体にインストールするようにしてもよい。また、このプログラムは、必ずしも単一に構成されるものに限られず、複数のモジュールやライブラリとして分散構成されていてもよいし、ＯＳ等の別個のプログラムと協働してその機能を達成するものであってもよい。

【００６３】

【発明の効果】以上説明したように、この発明のネットワーク中継装置（請求項１）は、第１中継手段が、プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化してプライベートネットワーク外に中継し、第２中継手段が、プライベートネットワーク外からのＵＤＰパケットをＥＳＰパケットにデカプセル化してプライベートネットワーク内に中継する。これにより、ＥＳＰパケット／ＵＤＰパケットのカプセル化およびデカプセル化をネットワーク中継装置でまとめて行うことができるため、プライベートネットワーク内とプライベートネットワーク外とのＩＰＳｅｃ通信を行う機能の実装および管理を容易化し、コストを低減することができる。

【００６４】また、この発明のデータ通信システム（請求項２）は、第１中継手段が、プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化してＩＰＳｅｃ装置宛てに中継し、第２中継手段が、ＩＰＳｅｃ装置からのＵＤＰパケットをＥＳＰパケットにデカプセル化してプライベートネットワーク内に中継し、デカプセル化手段が、第１中継手段からのＵＤＰパケットをＥＳＰパケットにデカプセル化し、ＥＳＰ受信処理手段が、デカプセル化手段がデカプセル化したＥＳＰパケットの受信処理を行い、送信手段が、プライベートネットワークにＥＳＰパケットを送信する場合、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信する。これにより、ＥＳＰパケット／ＵＤＰパケットのカプセル化およびデカプセル化をネットワーク中継装置でまとめて行うことができるため、プライベートネットワーク内とプライベートネットワーク外とのＩＰＳｅｃ通信を行う機能の実装および管理を容易化し、コストを低減することができる。

【００６５】また、この発明のデータ通信システム（請求項３）は、決定手段が、第１中継手段がカプセル化するＥＳＰパケットの送信元のＵＤＰポート番号を決定し、第１記憶手段が、送信元のプライベートアドレスお

よびＵＤＰポート番号を対応させて記憶し、第１中継手段が、決定手段が決定したＵＤＰポート番号をＵＤＰ送信ポート番号として用いてカプセル化を行い、第１記憶手段が記憶したＵＤＰポート番号をＵＤＰ宛先ポート番号とするＵＤＰパケットを第２中継手段が受信した後、該ＵＤＰポート番号に対応する送信元からのＥＳＰパケットのカプセル化を省略し、第２中継手段が、受信したＵＤＰパケットのＵＤＰ宛先ポート番号に対応するプライベートアドレス宛てに中継を行い、第２記憶手段が、デカプセル化手段がデカプセル化するＵＤＰパケットのＵＤＰ送信元ポート番号を記憶し、送信手段が、第２記憶手段が記憶したＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用いてカプセル化を行う。これにより、同一の送信元からのＥＳＰパケットのカプセル化を２回目以降省略して、ＵＤＰパケットへのカプセル化によるオーバヘッドを低減することができるため、通信効率を向上させることができる。

【００６６】また、この発明のデータ通信システム（請求項４）は、第１中継手段が、プライベートネットワーク内から送信されたＩＫＥネゴシエーション用のＵＤＰパケットをＩＰＳｅｃ装置宛てに中継する場合に該ＵＤＰパケットのＵＤＰ送信元ポート番号を決定して中継し、第１記憶手段が、ＵＤＰパケットの送信元のプライベートアドレスおよびＵＤＰ送信元ポート番号を対応させて記憶し、第２中継手段が、ＩＰＳｅｃ装置からのＵＤＰパケットをＥＳＰパケットにデカプセル化し、該ＵＤＰパケットのＵＤＰ宛先ポート番号に対応するプライベートアドレス宛てに中継し、第２記憶手段が、第１中継手段からのＵＤＰパケットのＵＤＰ送信元ポート番号を記憶し、送信手段が、プライベートネットワークにＥＳＰパケットを送信する場合、第２記憶手段が記憶したＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用い、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信する。これにより、ＵＤＰパケットからＥＳＰパケットへのデカプセル化をネットワーク中継装置でまとめて行うことができ、また、プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化する必要がなくなるため、プライベートネットワーク内とプライベートネットワーク外とのＩＰＳｅｃ通信を行う機能の実装および管理を容易化し、コストを低減することができ、また、通信効率を向上させることができる。

【００６７】また、この発明のデータ通信方法（請求項５）は、第１中継工程で、プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化してプライベートネットワーク外に中継し、第２中継工程で、プライベートネットワーク外からのＵＤＰパケットをＥＳＰパケットにデカプセル化してプライベートネットワーク内に中継する。これにより、ＥＳＰパケット／ＵＤＰパケットのカプセル化およびデカプセル化をまとめて行うことができるため、プライベートネットワーク内とプライベートネットワーク外とのＩＰＳｅｃ通信を行う機能の実装および管理を容易化し、コストを低減することができる。

【００６８】また、この発明のデータ通信方法（請求項６）は、第１中継工程で、プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化してプライベートネットワーク外に中継し、デカプセル化工程で、第１中継工程で中継されたＵＤＰパケットの宛先側で該ＵＤＰパケットをＥＳＰパケットにデカプセル化し、ＥＳＰ受信処理工程で、デカプセル化工程でデカプセル化されたＥＳＰパケットの受信処理を行い、送信工程で、宛先側からプライベートネットワークにＥＳＰパケットを送信する場合、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信し、第２中継工程で、送信工程で送信されたＵＤＰパケットをＥＳＰパケットにデカプセル化してプライベートネットワーク内に中継する。これにより、ＥＳＰパケット／ＵＤＰパケットのカプセル化およびデカプセル化をまとめて行うことができるため、プライベートネットワーク内とプライベートネットワーク外とのＩＰＳｅｃ通信を行う機能の実装および管理を容易化し、コストを低減することができる。

【００６９】また、この発明のデータ通信方法（請求項７）は、第１中継工程で、ＥＳＰパケットの送信元のＵＤＰポート番号を決定し、該ＵＤＰポート番号をＵＤＰ送信元ポート番号として用いてカプセル化を行い、該送信元のプライベートアドレスおよび該ＵＤＰポート番号を対応させて記憶し、該ＵＤＰポート番号をＵＤＰ宛先ポート番号とするＵＤＰパケットが第２中継工程で受信された後、該ＵＤＰポート番号に対応する送信元からのＥＳＰパケットのカプセル化を省略し、第２中継工程で、受信したＵＤＰパケットのＵＤＰ宛先ポート番号に対応するプライベートアドレス宛てに中継を行い、デカプセル化工程で、デカプセル化するＵＤＰパケットのＵＤＰ送信元ポート番号を記憶し、送信工程で、デカプセル化工程で記憶されたＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用いてカプセル化を行う。これにより、同一の送信元からのＥＳＰパケットのカプセル化を２回目以降省略して、ＵＤＰパケットへのカプセル化によるオーバヘッドを低減することができるため、通信効率を向上させることができる。

【００７０】また、この発明のデータ通信方法（請求項８）は、第１中継工程で、プライベートネットワーク内から送信されたＩＫＥネゴシエーション用のＵＤＰパケットを該プライベートネットワーク外に中継する場合、該ＵＤＰパケットのＵＤＰ送信元ポート番号を決定し、該ＵＤＰパケットの送信元のプライベートアドレスおよび該ＵＤＰ送信元ポート番号を対応させて記憶し、記憶工程で、第１中継工程で中継されたＵＤＰパケットの宛

先側で、該ＵＤＰパケットのＵＤＰ送信元ポート番号を記憶し、送信工程で、宛先側からプライベートネットワークにＥＳＰパケットを送信する場合、記憶工程で記憶されたＵＤＰ送信元ポート番号をＵＤＰ宛先ポート番号として用い、該ＥＳＰパケットをＵＤＰパケットにカプセル化して送信し、第２中継工程で、送信工程で送信されたＵＤＰパケットをＥＳＰパケットにデカプセル化し、該ＵＤＰパケットのＵＤＰ宛先ポートに対応するプライベートアドレス宛てに中継する。これにより、ＵＤＰパケットからＥＳＰパケットへのデカプセル化をまとめて行うことができ、また、プライベートネットワーク内から送信されたＥＳＰパケットをＵＤＰパケットにカプセル化する必要がなくなるため、プライベートネットワーク内とプライベートネットワーク外とのＩＰＳｅｃ通信を行う機能の実装および管理を容易化し、コストを低減することができ、また、通信効率を向上させることができる。

【００７１】また、この発明のプログラム（請求項９）は、前述した発明にかかる方法の動作をコンピュータによって実現することが可能となる、という効果を奏する。

【図面の簡単な説明】

【図１】この発明の一実施の形態にかかる通信ネットワークのシステム構成を示す説明図である。

【図２】図１に示したルータの機能構成を示すブロック図である。

【図３】図１に示したＩＰＳｅｃ装置の機能構成を示すブロック図である。

【図４】この実施の形態にかかるルータが外部ネットワークにパケットを送信する場合の動作手順を示すフローチャートである。

【図５】この実施の形態にかかるルータが受信するプライベートネットワーク内から送信されたＩＰパケットの一例を示す説明図である。

【図６】この実施の形態にかかるルータが記憶する変換情報の一例を示す説明図である。

【図７】この実施の形態にかかるＩＰヘッダのＮＡＴ変換後のＩＰパケットの一例を示す説明図である。

【図８】この実施の形態にかかるルータが外部ネットワークに送信するＩＰパケットの一例を示す説明図である。

【図９】この実施の形態にかかるＩＰＳｅｃ装置が外部ネットワークからのパケットを受信する場合の動作手順を示すフローチャートである。

【図１０】この実施の形態にかかるＩＰＳｅｃ装置が記憶する変換情報の一例を示す説明図である。

【図１１】この実施の形態にかかるＩＰＳｅｃ装置が記憶するＩＰＳｅｃ通信相手装置情報の一例を示す説明図である。

【図１２】この実施の形態にかかるＩＰＳｅｃ装置がセンターネットワーク内に送信するＩＰパケットの一例を示す説明図である。

【図１３】この実施の形態にかかるＩＰＳｅｃ装置が外部ネットワークにパケットを送信する場合の動作手順を示すフローチャートである。

【図１４】この実施の形態にかかるＩＰＳｅｃ装置が記憶するＩＰＳｅｃ通信対象パケット情報の一例を示す説明図である。

【図１５】この実施の形態にかかるＩＰＳｅｃ装置が受信するセンターネットワーク内から送信されたＩＰパケットの一例を示す説明図である。

【図１６】この実施の形態にかかるＩＰＳｅｃ装置が外部ネットワークに送信するＩＰパケットの一例を示す説明図である。

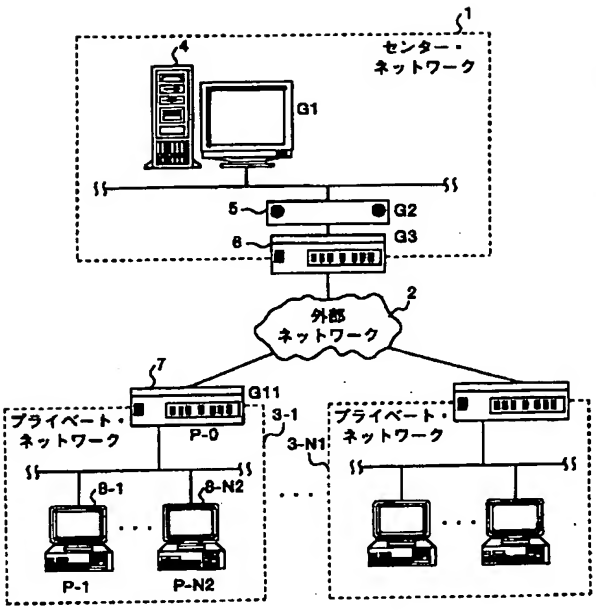
【図１７】この実施の形態にかかるルータが外部ネットワークからのＵＤＰパケットを受信する場合の動作手順を示すフローチャートである。

【図１８】この実施の形態にかかるルータがプライベートネットワーク内に送信するＩＰパケットの一例を示す説明図である。

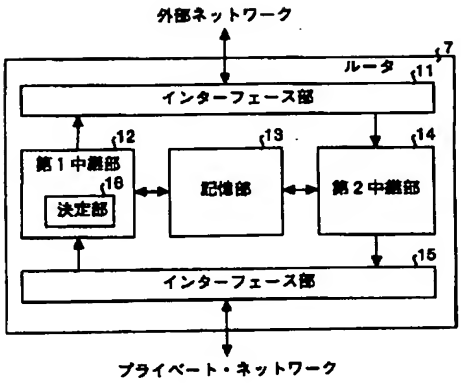
【符号の説明】

１　センターネットワーク
２　外部ネットワーク
３－１～３－Ｎ１　プライベートネットワーク
４　サーバ
５，８－１～８－Ｎ２　ＩＰＳｅｃ装置
６，７　ルータ
１１，１５，２１，２７　インターフェース部
１２　第１中継部
１３，２５　記憶部
１４　第２中継部
１６　決定部
２２　ＥＳＰ受信処理部
２３　ＥＳＰパケット生成部
２４　デカプセル化部
２６　送信部

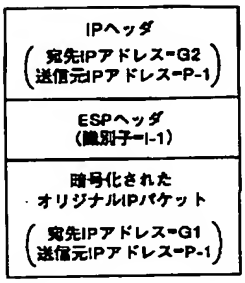
【図１】



【図２】



【図５】

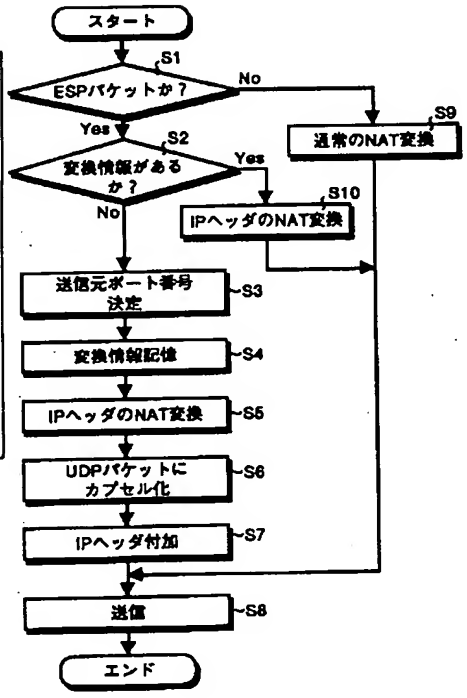


【図６】

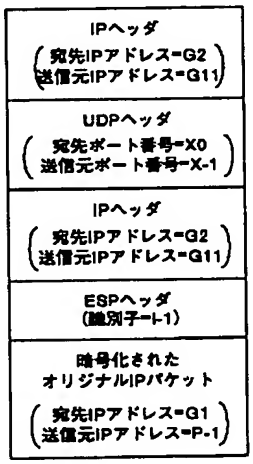
プライベートIPアドレス	ポート番号
P-1	X-1
P-2	X-2
⋮	⋮

【図３】

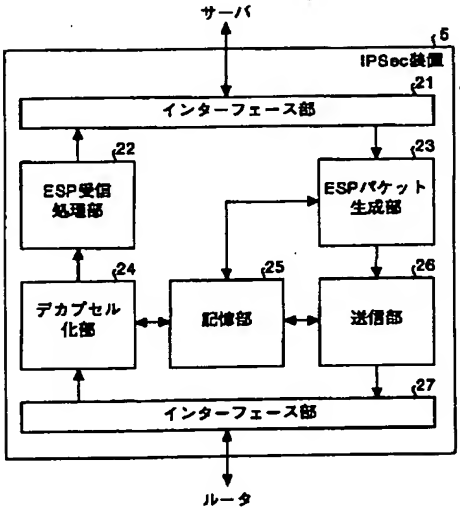
【図４】



【図８】



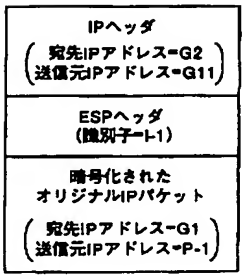
【図７】

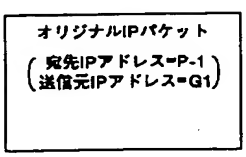


【図１０】

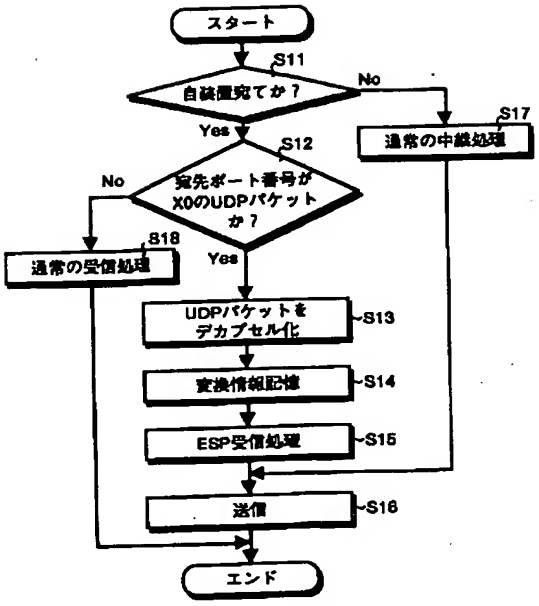
送信元装置	UDP送信元ポート番号
IPSec装置8-1	X-1
IPSec装置8-2	X-2
⋮	⋮

【図１５】





【図９】



【図１１】

相手装置	IPアドレス	識別子
IPSec装置B-1	G1	I-1
IPSec装置B-2	G1	I-2
⋮	⋮	⋮

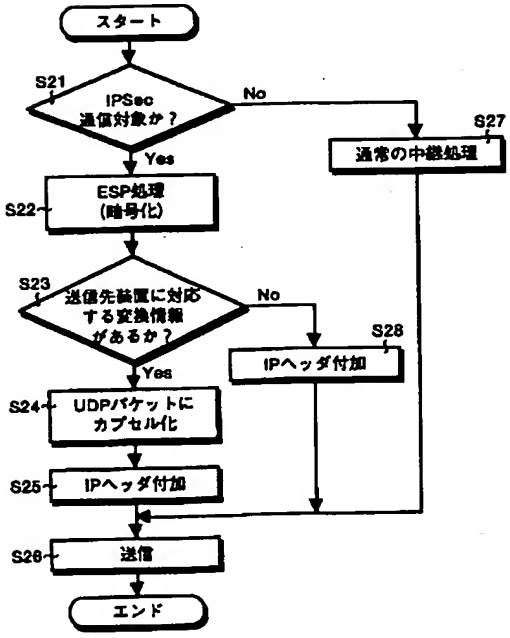
【図１２】

オリジナルIPパケット
（宛先IPアドレス=G1 送信元IPアドレス=P-1）

【図１８】

IPヘッダ（宛先IPアドレス=P-1 送信元IPアドレス=G2）
ESPヘッダ
暗号化されたオリジナルIPパケット（宛先IPアドレス=P-1 送信元IPアドレス=G1）

【図１３】



【図１４】

宛先IPアドレス／マスク	送信元IPアドレス／マスク	プロトコル	宛先ポート番号	送信元ポート番号	送信先装置
IPa	IPb	all	all	all	IPSec装置B-1
IPc	IPd	Prl	P-2	yy	IPSec装置B-2
・	・	・	・	・	・
・	・	・	・	・	・
・	・	・	・	・	・

【図１６】

IPヘッダ（宛先IPアドレス=G11 送信元IPアドレス=G2）
UDPヘッダ（宛先ポート番号=X-1 送信元ポート番号=X0）
ESPヘッダ
暗号化されたオリジナルIPパケット（宛先IPアドレス=P-1 送信元IPアドレス=G1）

【図１７】